

APPELLANT'S AMENDED BRIEF ON APPEAL UNDER 37 CFR § 1.192

SCULLY, SCOTT, MURPHY & PRESER
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

John F. Vodopia
Attorney for Appellant
Reg. No. 36,299

TABLE OF CONTENTS

	<u>PAGE</u>
I. REAL PARTY IN INTEREST	1
II. RELATED APPEALS AND INTERFERENCES	2
III. STATUS OF CLAIMS	2
IV. STATUS OF AMENDMENTS	3
V. SUMMARY OF CLAIMED SUBJECT MATTER	3
VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL	7
VII. ARGUMENT	8
A.) The combined disclosures of Lewis, Ellison and Brand do not render claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35, on appeal, unpatentable under 35 USC §103(a).	8
B.) The combined disclosures of Lewis, Muftic and Ellison do not render claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35, on appeal, unpatentable under 35 USC §103(a).	12
C.) The combined disclosures of Lewis, Ellison, Brand and Muftic do not render claims 12, 14-15 and 18, on appeal, unpatentable under 35 USC §103(a).	15
VII. CLAIMS APPENDIX	17
VIII. EVIDENCE APPENDIX	25
IX. RELATED PROCEEDINGS APPENDIX	26

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Elsie Van Herreweghen

Examiner: Jung W. Kim

Serial No: 09/899,444

Art Unit: 2132

Filed: July 5, 2001

Docket: CH920000009US1 (18907)

For: SECURE ANONYMOUS VERIFICATION
GENERATION AND/OR PROOF OF
OWNERSHIP OF ELECTRONIC RECEIPTS

Dated: August 10, 2007

Confirmation No: 4090

Mail Stop Appeals
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' AMENDED BRIEF ON APPEAL UNDER 37 C.F.R. §1.192

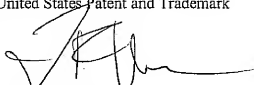
I. REAL PARTY IN INTEREST

The real party in interest of the present application is International Business Machines Corporation, the assignee of the entire right, title and interest in the above-identified patent application.

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited with the United States Patent & Trademark Office via Electronic Filing through the United States Patent and Trademark Office e-business website, on the date shown below.

Dated: August 10, 2007



John F. Vodopia

II. RELATED APPEALS AND INTERFERENCES

No other appeals or interferences are known which directly affect, or will be directly affected by, or have a bearing on, the disposition of the pending appeal.

III. STATUS OF THE CLAIMS

The present application was filed on July 5, 2001 with claims 1-35. A first Office Action on the merits issued on February 24, 2005, to which appellant filed an Amendment (Under 37 CFR 1.111) on June 22, 2005. In the June 22, 2005, Amendment, claims 1, 6, 13, 21, 24, 25 and 26 were amended. A Final Rejection dated August 1, 2005, was then issued to which appellant filed an Amendment under 37 C.F.R. §1.116, on September 15, 2005, wherein claims 1, 6, 13, 24-26 were amended. An Advisory Action then issued on October 5, 2005, indicating that the claims amendments set forth in appellants' Amendment Under 37 CFR 1.116, filed September 15, 2005, would not be entered since it raised new issues that would require further consideration and/or searching.

A Request For Continued Examination (RCE) was filed on November 1, 2005, requesting entry of the un-entered Amendment Under 37 CFR 1.116 (of September 15, 2005). An Office Action dated December 20, 2005, was issued pursuant to the RCE filing entering the previously un-entered amendment. In response to the December 20, 2005, Office Action, appellants filed an Amendment (Under 37 CFR 1.111) on March 20, 2006, wherein claims 1, 6, 13 and 24-26 were amended. Despite those amendments, another Final Rejection dated April 14, 2006, was issued. In response to that Final Rejection, appellants submitted a Response under 37 C.F.R. §1.116, dated June 14, 2006, again amending claims 1, 6, 13 and 24-26. An Advisory Action dated June 27, 2006, was issued, which indicated that appellant's Amendment Under 37 CFR 1.116 dated June 27, 2006, would not be entered.

An RCE was filed on July 14, 2006, requesting entry of the un-entered Amendment Under 37 CFR 1.116, previously filed on June 14, 2006. An Office Action issued on August 30, 2006, in response to the RCE, entering and responding to the previously un-entered

Amendment Under 37 CFR 1.116. In response to the August 30, 2006, Office Action, appellant filed an Amendment (Under 37 CFR 1.111), dated November 15, 2006, wherein claims 1, 6, 13 and 24-26 were amended. Despite these amendments, another final Office Action finally rejecting each of pending claims 1-28 and 30-35, issued January 12, 2007. In response to the final rejection dated January 12, 2007, applicants filed an Amendment Under 37 CFR 1.116, on March 12, 2007. In the final Amendment, none of pending claims 1-28 and 30-35 were amended.

An Advisory Action issued on April 3, 2007, maintaining the final rejections. In reply to the Advisory Action, a Notice of Appeal was mailed to the United States Patent and Trademark Office on April 12, 2007. Subsequent to the filing of the Notice of Appeal on April 12, 2007, applicant filed a Supplemental Amendment Under 37 CFR 1.116, on June 6, 2007, in order to cancel claim 16, which claim was objected to in the last final Office Action.

Thus, the status of each of the pending claims 1-15, 17-28 and 30-35 is that they are finally rejected and on appeal, where claims 1, 6, 13 and 24-26 are the independent claims.

IV. STATUS OF THE AMENDMENTS

An Amendment under 37 C.F.R. §1.116, in response to the Final Rejection dated January 12, 2007, including arguments for patentability was filed on March 12, 2007, and Supplemental Amendment under 37 CFR 1.116, filed June 6, 2007, canceling claim 16 to place the application in proper condition for appeal. Appellants' Amendment under 37 C.F.R. §1.116 was entered and considered by way of the Advisory Action dated April 3, 2007, and applicant's Supplemental Amendment Under 37 CFR 1.116, canceling claim 16, is believed to be entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1-15, 17-28 and 30-35 are the pending claims on appeal; claims 1, 6, 13 and 24-26, are the independent claims. Pending dependent claims 2-5 and 30 depend from claim

1, dependent claims 7-12, 27 and 31 depend from claim 6, dependent claims 14, 15 and 17-23, 28 and 32 depend from claim 13, dependent claim 33 depends from claim 24, dependent claim 34 depends from claim 25 and dependent claim 35 depends from claim 26. All of the claims on appeal will stand or fall together based on the patentability of independent claims 1, 6, 13 and 24-26.

The invention with respect to independent claim 1 comprises a verification method comprising verifying ownership of an electronic receipt in a communication system (Fig. 1) providing a public key encryption infrastructure (page 5, lines 4-7). The verification method includes steps of receiving a message from a sender (page 7, lines 6-9), said message being electronically signed by said sender (100) using a first private signature key of a first private-public key pair owned by said sender (page 7, lines 9-11), wherein said message includes the electronic receipt as electronically signed by an issuer (106) using a private signature key of a second private-public key pair that is assigned to the issuer (page 7, lines line 26-30), and wherein the receipt includes details for what said receipt has been given and a reference to a designated owner of the receipt (page 7, lines 16-20); obtaining a public signature verification key on the basis of said reference to said owner of the electronic receipt (page 8, lines 1-7); and examining whether or not said second private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt thereby to verify ownership of the receipt by said owner while maintaining said owner anonymous or pseudonymous (110; page 8, lines 1-10).

The invention with respect to independent claim 6 comprises a receipt generation method, comprising generating an electronic receipt in a communication system (Fig. 1) providing a public key encryption system, and including steps of receiving a message from a sender (100) using a pseudonym (page 10, lines 10-13), wherein said pseudonym is issued using a first private-public signature key pair (page 11, lines 30-32), and said message is electronically signed by said sender using the first private signature key owned by said sender (page 11, line 32-page 12, line 1), whereby said message includes a transaction request and a reference to a designated owner of a receipt to be generated (page 12, lines 2-3);

authenticating said message using a public signature verification key associated to said first private signature key held by said sender of said message (110; page 13, lines 10-29); issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given to provide said designated owner with said receipt and thereby to enable said owner to verify ownership of the receipt by using a second private-public signature key pair different than the first private-public signature key pair, while maintaining said owner anonymous or pseudonymous (page 14, lines 7-12); and electronically signing and issuing said receipt using the second private-public signature key pair assigned to an issuer issuing said receipt (page 18, lines 6-16).

The invention with respect to independent claim 13 comprises a method for proving ownership of a receipt, the method comprising proving ownership of said receipt in a communication system (Fig. 1) providing a public key encryption infrastructure, including steps of a user (100) using a pseudonym to create a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving said message (page 10, lines 10-13), wherein said pseudonym is issued to the user (100) using a first private-public signature key pair; the user electronically signing said message using the first private signature key (page 11, lines 30-32); sending said first message to a first addressee; and receiving said receipt from said first addressee, said receipt being electronically signed by said first addressee using a second private signature key of a second private-public key pair assigned to said first addressee (page 11, line 32-page 12, line 1), wherein said receipt includes information as for what said receipt has been issued and said reference to said designated owner of said receipt and thereby to enable said owner to verify ownership of the receipt by using the second private-public signature key pair different than the first private-public signature key pair, while maintaining said owner anonymous or pseudonymous (page 14, lines 7-12).

The invention with respect to independent claim 24 comprises a verification device, the verification device comprising means (108; 106) for using a first private-public signature key pair to issue a pseudonym to a user (page 7, line 5-page 8, line 10); means (108; 100) for said user, using said pseudonym, to obtain a receipt that is electronically signed by an issuer

using a second private signature key of a second private-public signature key pair, and includes details for what said means for receiving a message from a sender that is electronically signed by said sender using the second private signature key that is different than the first private signature key and owned by said sender, said message includes said receipt (102, Fig. 1); means (116) for obtaining a public signature verification key of said second private-public signature key pair on the basis of said reference to said owner of said receipt (106, Fig. 1); and means (114) for examining whether or not said second private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt thereby to verify ownership of the receipt by said owner while maintaining said owner anonymous or pseudonymous, said device being for verifying ownership of said receipt in a communication system providing a public key encryption infrastructure (110, Fig. 1).

The invention with respect to independent claim 25 comprises a receipt generating device, the receipt generating device comprising means (104; 102) for receiving a message from a sender using a pseudonym (page 7, line 5-page 8, line 10), wherein said pseudonym is issued using a first private-public signature key pair, and said message is electronically signed by said sender using a second private signature key of a second private-public signature key pair owned by said sender, and wherein said message includes a transaction request and a reference to a designated owner of a receipt to be generated (102, Fig. 1); means (112; 110) for authenticating said message using a first public signature verification key associated to said first private signature key held by said sender of said message (102, Fig. 1); means (104; 102) for issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given to provide said designated owner with said receipt and enable said owner to verify ownership of the receipt using the second private-public signature key pair while maintaining said owner anonymous or pseudonymous; and means (202) for electronically signing said receipt with the second private signature key of the second private-public key pair assigned to an issuer issuing said receipt, said device being for generating said receipt in a communication system providing a public key encryption system (110, Fig. 1).

The invention with respect to independent claim 26 comprises a device for proving ownership of a receipt, said device comprising means (104; 100) for a user, using a pseudonym, for creating a first message including a transaction request and a reference to a designated owner of the receipt to be generated in response of receiving said message, wherein said pseudonym is issued using a first private-public signature key pair; means (202) for electronically signing said message by the user using the first private signature key (page 7, line 5-page 8, line 10); means for sending said first message to a first addressee; means (116; 108; 106) for receiving a receipt from said first addressee, which is electronically signed by said first addressee having given said receipt using a second private signature key of a second private-public signature key pair assigned to said first addressee (102, Fig. 1), wherein said receipt includes information related to a purpose for which said receipt has been given, and related to said reference to said designated owner of said receipt thereby to enable said owner to verify ownership of the receipt by said owner by using the second private-public signature key pair while maintaining said owner anonymous or pseudonymous, said device being for proving ownership of the receipt in a communication system providing a public key encryption infrastructure (110, Fig. 1).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A.) Do the combined disclosures of U.S. Patent No. 6,233,565 to Lewis, et al. ("Lewis"), U.S. Patent No. 6,976,162 to Ellison, et al. ("Ellison"), and U.S. Patent No. 5,604,805 to Brand ("Brand") render claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35, on appeal, unpatentable under 35 USC §103(a)?

B.) Do the combined disclosures of Lewis, Ellison and US Patent No. 5,850,442 to Muftic ("Muftic") render claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35, on appeal, unpatentable under 35 USC §103(a)?

C.) Do the combined disclosures of Lewis, Ellison, Brand and Muftic render claims 12, 14-15 and 18, on appeal, unpatentable under 35 USC §103(a)?

VII. Argument

A.) The combined disclosures Lewis, Ellison and Brand do not render claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35, unpatentable under 35 USC §103(a).

This obviousness rejection under 35 U.S.C. 103 relies on the proposed combined teachings of Lewis, Ellison and Brand for allegedly disclosing appellant's invention as set forth in claims 6-11, 13, 17, 19-22, 25-28, 31, 32, 34 and 35. Appellant respectfully submits, however, that the present claims on appeal are not obvious from the above proposed combination of references since none of them teaches or suggests appellant's claimed receipt generation method (independent claim 6), method for proving ownership of a receipt (independent claim 13), receipt generating device (independent claim 25) and device for providing ownership of a receipt (independent claim 26).

More particularly with respect to independent claims 6, 13, 25 and 26, there is no teaching, suggestion or motivation found in any of Lewis, Ellison or Brand that would have rendered the proposed combination, or appellant's invention as claimed, obvious to the skilled artisan under 35 USC §103(a). The Examiner states with respect to the rejection of claim 6 that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to use a second private-public signature key pair different than the first private-public signature key pair to verify ownership of the receipt, while maintaining the owner anonymous or pseudonymous" to "ensure better privacy for the user since the organization generating the receipt and the organization validating the ownership of the receipt are not able to collude to identify the owner of the receipt, Brand, *ibid*. The aforementioned covers the limitations of claim 6." The Examiner, however, is mistaken.

With respect to the rejection of independent claim 13 based on the same proposed combination of Lewis, Ellison and Brand, the Examiner states that the combination would have been obvious to maintain the anonymity of the owner, "since it is desirable to maintain the privacy of a user transferring certified information. The aforementioned cover the limitations of claim 13." With respect to the rejection of independent claims 25 and 26, the

Examiner asserts the same TSM. That is, appellant understands that the stated reasons asserted to render obvious claims 6, 13, 25 and 26, in view of the proposed combination are merely broad statements articulating the benefits of applicant's inventive subject matter using hindsight. The Examiner has not identified specific reasons found in any of the references that would have sufficiently prompted the skilled artisan to combine the three prior art references. KSR Int'l. Co. v. Teleflex, Inc., Slip Op. No. 04-1350 (US April 30, 2007). Appellant respectfully asserts that each of the references and the claimed invention may be said to be intended to keep private certified information transfers, but that applicant's claim language is not so broad as to merely set forth a receipt generation method to maintain the privacy of a user transferring certified information (independent claim 6), method for proving ownership of a receipt and maintaining the privacy of a user transferring certified information (independent claim 13), receipt generating device and maintaining the privacy of a user transferring certified information (independent claim 25) and device for providing ownership of a receipt and maintaining the privacy of a user transferring certified information (independent claim 26).

While appellant finds the stated reasons asserted by the Examiner that would compel the skilled artisan to make such a three-reference combination to be improper under Section 103(a) and KSR, even *assuming arguendo* that the stated reason to combine the three (3) references is proper, the proposed combination would still not render obvious rejected independent claims 6, 13, 25 and 26. That is, the proposed combination of Lewis, Ellison and Brand as asserted by the Examiner does not include each of the elements of the rejected claims, rendering the rejections improper. Appellant, therefore, respectfully requests that the rejection of independent claims 6, 13, 25 and 26 should be reversed by the Board of Patent Appeals and Interferences, for at least the following reasons.

Lewis is the primary reference relied on by the Examiner to reject the claims. Lewis describes procedures for issuing receipts over the Internet. The Lewis system includes that goods or services are purchased by a user over the Internet from a server having a receipt generation module, an authentication module and a transaction module. Special transaction software is used to manage the printing of various communications. The procedure disclosed

in Lewis is relatively standard in many respects, except that it is done using the Internet. Importantly, Lewis does not disclose any specific mechanism to keep the owner anonymous or pseudonymous, still less using a first and second private-public key pair to practice the invention disclosed therein.

As the Examiner has recognized, there are a number of important features of the preferred embodiment of the invention as included in independent claims 6, 13, 25 and 26 that are not shown in or suggested by Lewis (See outstanding final Office Action mailed January 12, 2007). Lewis at col. 4, lines 24-27, cols 7 and 8 refers to a transaction module that responds to a client and server being authenticated, and then the client issuing a transaction request to a server and transaction server, but nowhere suggests the use of a pair of private/public key pairs to maintain the user anonymous or pseudonymous.

In order to remedy this deficiency of Lewis as a reference, and hold the claims rejected under 35 USC 103(a) unpatentable, the Examiner relies on the additional references, including Ellison and Brand (and including Muftic, Ellison and Brand with respect to the rejections of independent claims 1 and 24, discussed below). None of Ellison and Brand overcome Lewis' shortcomings with respect to independent claims 6, 13, 25 and 26. That is, combining Ellison and Brand with Lewis does not realize the subject matter of applicant's independent claims 6, 13, 25 and 26.

Ellison merely describes a procedure for issuing a pseudonym to protect the identity of a platform and its use. At col. 3, lines 8-13, col. 3, line 57 through col. 5, line 9, Ellison describes the inventive operation. At a user request, a first platform 110 generates and transmits a pseudonym public key 140 to a second platform 120, which is responsible for certifying that the public key was generated by a trusted device 150 within the first platform. Once the Ellison platform receives this pseudonym, subsequent communications can be performed using the pseudonym to help keep the real identity of the platform anonymous. Ellison does not mention, teach or suggest using a first and a second private-public key pair to practice the invention disclosed therein. For that matter, this teaches away from appellant's invention as set forth in the subject matter of independent claims 6, 13, 25 and 26.

Brand describes use of a restrictive blind signature protocol in combination with a testing protocol in order that certified information may be transferred in a “blinded” way, to ensure untraceability. Brand at col. 2, lines 15-34, discusses a conventional second cryptographic concept to “guarantee” privacy of users when transferring certified information. The known method includes allowing users to be known by different pseudonyms at different organization such that the pseudonyms are unlinkable (a blind signature protocol. In this way, information certified by a particular organization can be shown to all other organizations at which the user has a pseudonym without enabling the other organizations to link the transferred information. Brand does not mention, teach or suggest using first and second private-public key pairs to practice the invention disclosed therein. For that matter, this Brand appears to teach away from appellant’s invention as set forth in the subject matter of independent claims 6, 13, 25 and 26.

Appellant respectfully asserts, therefore, that Lewis combined with Ellison, and Lewis and Ellison combined with Brand, whether alone or in combination, do not teach or suggest how to issue and to verify ownership of a receipt while maintaining the owner anonymous or pseudonymous, still less using first and second private-public signature key pairs, where a user and receipt issuer exchange information using the first private-public key pair, and the receipt issuer and owner communicate using the second private-public key pair, which are limitations set forth in each of appellant’s independent claims 6, 13, 25 and 26.

Because of the above-discussed differences between independent claims 6, 13, 25 and 26, and because of the advantages associated with those differences, appellant urges that these claims patentably distinguish over the proposed prior art combination of Lewis, Ellison and Brand, and are allowable under Section 103(a). Claims 7-11 and 31 depend from claim 6 and are patentable therefore; claims 17, 19-22, 28 and 32 depend from claim 13, and patentable therefore; claim 34 is patentable in view of its dependency from claim 25, and claim 35 by its dependency from claim 26. The Board of Patent Appeals and Interferences is therefore respectfully requested to reverse the above-identified rejections of claims 6-11,13,17,19-22,

25-28, 31, 32, 34 and 35 under Section 103(a) by the Lewis/Ellison/Brand combination, and to allow these claims.

B.) The combined disclosures of Lewis, Muftic and Ellison do not render claims 1-5, 23, 24, 30 and 33, unpatentable under 35 USC §103(a)

This obviousness rejection under 35 U.S.C. 103(a) relies on the combined teachings of Lewis, Muftic and Ellison for allegedly disclosing applicant's invention as set forth in claims 1-5, 23, 24, 30 and 33. Appellant respectfully submits that the present claims on appeal, are not obvious in view of the proposed combination of Lewis, Muftic and Ellison, since none of the applied references teaches or suggests appellant's claimed verification method (independent claim 1), and verification device (independent claim 24).

More particularly with respect to independent claims 1 and 24, appellant asserts that there is no teaching, suggestion or motivation found in any of Lewis, Muftic or Ellison that would have motivated the skilled artisan to make such a combination, or otherwise render applicant's invention as claimed obvious to the skilled artisan under 35 USC §103(a). The Examiner states with respect to the rejection of claims 1 and 24 that "it would be obvious to one of ordinary skill in the art at the time the invention was made for the reference to the owner of the receipt to be a pseudonym used by the owner of the receipt and a certificate to securely link the pseudonym to the public signature verification key, such that the verification of ownership of the receipt is enable while maintaining the owner anonymous or pseudonymous, since it is desirous to maintain the privacy of a user transferring certified information," citing Ellison at 1:65-2:1.

Appellant, however, strongly disagrees because she finds that that the cited Ellison text merely recites protecting the identity of a platform through the use of pseudonyms. For that matter, the Examiner asserts that, "although Muftic does not teach submitting a certificate holding the public signature verification key and signed by the issuer with the original signed message, the step of including the certificate with the signed message is a trivial combination since proper verification of the signed message requires the signed certificate, citing Muftic at

col. 3, lines 30-33, and concludes that appellant's claims 1 and 24 are merely combinations of disparate parts. Appellant respectfully asserts that the Examiner is mistaken. Appellant understands that the stated reasons to render obvious claims 1 and 24 by the proposed combination are merely broad statements articulating the benefits of applicant's inventive subject matter using hindsight, but are not proper under 35 USC §103(a) or KSR. The Examiner has not identified reasons found in any of the references that would have sufficiently prompted the skilled artisan to combine the three prior art references. KSR Int'l. Co. v. Teleflex, Inc., Slip Op. No. 04-1350 (US April 30, 2007).

But even *assuming arguendo* that there is some teaching, suggestion or motivation to combine that could render the proposed combination of the three (3) references proper, the proposed combination would still not render obvious rejected independent claims 1 and 24. The combination of Lewis, Muftic and Ellison is not found to include each of the elements of the rejected claims, so the rejection of claims 1 and 24 should be reversed by the Board of Patent Appeals and Interferences, for at least the following reasons.

Lewis, as described above, is the primary reference relied on by the Examiner. Lewis describes procedures for issuing receipts over the Internet, including those goods or services are purchased by a user (over the Internet) from a server having a receipt generation module. Special transaction software is used to manage the printing of various communications, but as already mentioned, does not disclose any specific mechanism to keep the owner anonymous or pseudonymous, nor teach or suggest using first and second private-public key pairs to practice the invention disclosed therein.

Muftic was cited in the Office Action for its disclosure of a method and system for performing secure electronic commerce. In the Muftic method and system disclosed, procedures are used to authenticate signed messages. Muftic discloses procedures to authenticate signed messages, which is distinguished from the operation of applicant's invention as set forth in independent claim 1 and 14 that is directed to maintaining the transaction in confidentiality. Muftic at col. 2, lines 42-51, col. 3, lines 35-52 and col. 4, lines 27-32 states that messages are signed by first creating a message digest, and encrypting the

message digest using a signer's private key. Authentication that the content of the document has not been changed is achieved by computing the message digest of the received text and comparing it to the message digest decrypted using the signer's public key. It is important to note that this reference is directed primarily to authentication rather than to confidentiality (emphasis added). Muftic does not mention, teach or suggest using first and second private-public key pairs to practice the invention disclosed therein.

Brand, as described above, teaches the use of a restrictive blind signature protocol in combination with a testing protocol in order that certified information may be transferred in a "blinded" way, to ensure untraceability, but does not mention, teach or suggest using first and second private-public key pairs to practice a verification method as set forth in appellant's independent claim 1, or a verification device as set forth in appellant's independent claim 24.

Applicant respectfully asserts, therefore, that Lewis combined with Muftic, the proposed Lewis/Muftic combination combined with Ellison, whether alone or in combination, does not disclose a verification method, or a verification device, both claimed inventions arranged to issue and verify ownership of a receipt while maintaining the owner anonymous or pseudonymous, still less issuing and verifying ownership of a receipt using first and second private-public signature key pairs, where a user and receipt issuer exchange information using the first private-public key pair, and the receipt issuer and owner communicate using the second private-public key pair, as set forth in each of appellant's independent claims 1 and 24.

Because of the above-discussed differences between independent claims 1 and 24, and because of the advantages associated with those differences, these claims patentably distinguish over the proposed combination of Lewis, Muftic and Brands, and are allowable under Section 103(a). Claims 2-5, 23 and 30 are dependent from claim 1 and are allowable therewith; and claim 33 is dependent from claim 24 and patentable therewith. The Board of Patent Appeals and Interferences is therefore respectfully requested to reverse the above-identified rejections of claims 1-5, 23, 24, 30 and 33 under Section 103(a) by the Lewis/Muftic/Brand combination, and to allow these claims.

C.) The combined disclosures of Lewis, Ellison, Brand and Muftic do not render claims 12, 14-15 and 18, on appeal, unpatentable under 35 USC §103(a)

This obviousness rejection under 35 U.S.C. 103(a) relies on the combined teachings of Lewis, Ellison, Brand and Muftic for allegedly disclosing applicant's invention as set forth in dependent claims 12, 14-15 and 18. Appellant respectfully submits that the present claims, on appeal, are not obvious in view of the proposed combination of Lewis, Ellison, Brand and Muftic since none of the applied references teaches or suggests appellant's claimed receipt generation method of independent claim 6, from which claim 12 depends, and independent claim 13, from which claims 14-15 and 18 depend.

More particularly with respect to claims 12, 14-15 and 18, appellant asserts that there is no teaching or suggestion found in any of Lewis, Ellison, Brand or Muftic that would motivate the skilled artisan to make such a combination of the four (4) references. While the Examiner asserts that "as disclosed by Muftic, public keys are conventionally certified by means of a certificate to associate a signature key with a subscriber (col. 2, lines 42-51, col. 3, lines 35-52 and col. 4, lines 27-32," and that it would have been obvious therefore for the skilled artisan to have realized the proposed combination of the four (4) references for the reference to a designated owner to be a public signature key associated to a private signature key held by the designated owner of the receipt, because it enables a certified reference to the signed receipt, appellant respectfully asserts that such statements fall short in establishing that the dependent claims are obvious in view of said proposed by-four combination of references under the law. (See language of appellant's independent claims 6 and 13).

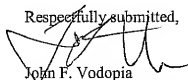
But even *assuming arguendo* that there is some teaching, suggestion or motivation to combine the four (4) references that could render the proposed combination proper under 35 USC §103(a) and KSR, the proposed combination would still not render obvious the rejected dependent claims for at least the reasons set forth above for the patentability of independent

claims 6 and 13 under Section 103(a) in view of Lewis, Ellison and Brand, from which claims the rejected dependent claims depend.

The combination of Lewis, Ellison, Brand and Muftic is not found to include each of the elements of the rejected claims. That is, the proposed combination does not teach or suggest how to issue and to verify ownership of a receipt while maintaining the owner anonymous or pseudonymous, still less using first and second private-public signature key pairs, where a user and receipt issuer exchange information using the first private-public key pair, and the receipt issuer and owner communicate using the second private-public key pair, which are limitations set forth in each of appellant's independent claims 6, 13, so the rejection of claims 12, 14-15 and 18, cannot be maintained under the law of 35 USC §103(a), and should be reversed by the Board of Patent Appeals and Interferences.

Because of the above-discussed differences between dependent claims 12, 14-15 and 18, because of the advantages associated with those differences, and in view of the arguments for patentability under Section 103 for patentability of the claims from which rejected claims 12 and 14-15 depend, those dependent claims patentably distinguish over the prior art and are allowable. The Board of Patent Appeals and Interferences is therefore respectfully asked to reconsider and to reverse the rejections of claims 12, 14-15 and 18 by the combination of Lewis, Ellison, Brand and Muftic, and to allow these claims.

Respectfully submitted,



John F. Vodopia
Registration No. 36, 299
Attorney for Applicant

SCULLY, SCOTT, MURPHY & PRESER, P.C.
400 Garden City Plaza, Suite 300
Garden City, New York 11530
(516) 742-4343

JFV:gc

VIII. CLAIMS APPENDIX

The claims on appeal for U.S. Application Serial No. 09/070,394, filed April 30, 1998:

1. (Previously Presented) A verification method comprising verifying ownership of an electronic receipt in a communication system providing a public key encryption infrastructure, including the steps of:
 - receiving a message from a sender, said message being electronically signed by said sender using a first private signature key of a first private-public key pair owned by said sender, wherein said message includes the electronic receipt as electronically signed by an issuer using a private signature key of a second private-public key pair that is assigned to the issuer, and wherein the receipt includes details for what said receipt has been given and a reference to a designated owner of the receipt;
 - obtaining a public signature verification key on the basis of said reference to said owner of the electronic receipt; and
 - examining whether or not said second private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt thereby to verify ownership of the receipt by said owner while maintaining said owner anonymous or pseudonymous.
2. (Original) The method according to claim 1, wherein said reference to said owner of said receipt is a public signature verification key associated to a private signature key held by said owner of said receipt.
3. (Original) The method according to claim 1, wherein said reference to said owner of said receipt is a pseudonym used by said owner of the receipt.

4. (Original) The method according to claim 3, wherein obtaining said public signature verification key on the basis of said pseudonym used by said owner of said receipt includes getting a certificate securely linking said pseudonym to said public signature verification key.
5. (Original) The method according to claim 1, further comprising the step of authenticating said receipt using a public signature verification key assigned to said issuer of said receipt.
6. (Previously Presented) A receipt generation method, comprising generating an electronic receipt in a communication system providing a public key encryption system, including the steps of:
 - receiving a message from a sender using a pseudonym, wherein said pseudonym is issued using a first private-public signature key pair, and said message is electronically signed by said sender using the first private signature key owned by said sender, whereby said message includes a transaction request and a reference to a designated owner of a receipt to be generated;
 - authenticating said message using a public signature verification key associated to said first private signature key held by said sender of said message;
 - issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given to provide said designated owner with said receipt and thereby to enable said owner to verify ownership of the receipt by using a second private-public signature key pair different than the first private-public signature key pair, while maintaining said owner anonymous or pseudonymous; and
 - electronically signing and issuing said receipt using the second private-public signature key pair assigned to an issuer issuing said receipt.
7. (Original) The method according to claim 6, further including the steps of performing said requested transaction, and returning said receipt to said sender.

8. (Original) The method according to claim 6, wherein said sender uses an anonymous communication connection.
9. (Original) The method according to claim 6, wherein said sender uses a pseudonym for communicating.
10. (Original) The method according to claim 6, wherein said reference to a designated owner is a pseudonym used by said designated owner.
11. (Original) The method according to claim 6, wherein said designated owner of the receipt is the sender.
12. (Original) The method according to claim 6, wherein said reference to a designated owner is a public signature key associated to a private signature verification key held by said designated owner of said receipt.
13. (Previously Presented) A method for proving ownership of a receipt, the method comprising proving ownership of said receipt in a communication system providing a public key encryption infrastructure, including the steps of:
 - a user using a pseudonym to create a first message including a transaction request and a reference to a designated owner of a receipt to be generated in response to receiving said message, wherein said pseudonym is issued to the user using a first private-public signature key pair;
 - the user electronically signing said message using the first private signature key;
 - sending said first message to a first addressee; and
 - receiving said receipt from said first addressee, said receipt being electronically signed by said first addressee using a second private signature key of a second private-public key pair assigned to said first addressee, wherein said receipt includes information as for what said receipt has been issued and said reference to said designated owner of said receipt and thereby to enable said owner to verify ownership

of the receipt by using the second private-public signature key pair different that the first private-public signature key pair, while maintaining said owner anonymous or pseudonymous.

14. (Original) The method according to claim 13, further comprising:
creating a second message including said receipt;
electronically signing said second message using a second private signature key; and
sending said second message to a second addressee;
15. (Previously Presented) The method according to claim 14, wherein the first addressee is identical to the second addressee.
16. (Cancelled)
17. (Original) The method according to claim 13, wherein said reference to said designated owner of said receipt is a pseudonym used by said owner of the receipt.
18. (Original) The method according to claim 13, wherein said reference to said designated owner of said receipt is a public signature verification key associated to a private signature key held by said owner of said receipt.
19. (Original) The method according to claims 13, wherein said designated owner of said receipt is identical to a sender sending said first message to the first addressee.
20. (Original) The method according to claim 13, further comprising:
creating a second message including said receipt; electronically signing said second message using a second private signature key; and
sending said second message to said designated owner of said receipt.

21. (Previously Presented) The method according to claim 20, wherein said steps of sending and receiving of the first message and second message is performed over an anonymous communication connection.
22. (Previously Presented) The method according to claim 20, wherein said sending and receiving of the first message and second message is performed by using a pseudonym.
23. (Original) A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 1.
24. (Previously Presented) A verification device comprising:
means for using a first private-public signature key pair to issue a pseudonym to a user;
means for said user, using said pseudonym, to obtain a receipt that is electronically signed by an issuer using a second private signature key of a second private-public signature key pair, and includes details for what said receipt has been given and a reference to a designated owner of said receipt;
means for receiving a message from a sender that is electronically signed by said sender using the second private signature key that is different than the first private signature key and owned by said sender, said message includes said receipt;
means for obtaining a public signature verification key of said second private-public signature key pair on the basis of said reference to said owner of said receipt;
and
means for examining whether or not said second private signature key used for electronically signing said message is associated to said public signature verification key obtained on the basis of said reference to said owner of said receipt thereby to verify ownership of the receipt by said owner while maintaining said owner anonymous or pseudonymous, said device being for verifying ownership of said receipt in a communication system providing a public key encryption infrastructure.

25. (Previously Presented) A receipt generating device comprising:

means for receiving a message from a sender using a pseudonym, wherein said pseudonym is issued using a first private-public signature key pair, and said message is electronically signed by said sender using a second private signature key of a second private-public signature key pair owned by said sender, and wherein said message includes a transaction request and a reference to a designated owner of a receipt to be generated;

means for authenticating said message using a first public signature verification key associated to said first private signature key held by said sender of said message;

means for issuing a receipt including said reference to said designated owner of said receipt and details for what said receipt has been given to provide said designated owner with said receipt and enable said owner to verify ownership of the receipt using the second private-public signature key pair while maintaining said owner anonymous or pseudonymous; and

means for electronically signing said receipt with the second private signature key of the second private-public key pair assigned to an issuer issuing said receipt, said device being for generating said receipt in a communication system providing a public key encryption system.

26. (Previously Presented) A device for proving ownership of a receipt, said device comprising:

means for a user, using a pseudonym, for creating a first message including a transaction request and a reference to a designated owner of the receipt to be generated in response of receiving said message, wherein said pseudonym is issued using a first private-public signature key pair;

means for electronically signing said message by the user using the first private signature key;

means for sending said first message to a first addressee;

means for receiving a receipt from said first addressee, which is electronically signed by said first addressee having given said receipt using a second private signature key of a second private-public signature key pair assigned to said first addressee, wherein said receipt includes information related to a purpose for which said receipt has been given, and related to said reference to said designated owner of said receipt thereby to enable said owner to verify ownership of the receipt by said owner by using the second private-public signature key pair while maintaining said owner anonymous or pseudonymous,

said device being for proving ownership of the receipt in a communication system providing a public key encryption infrastructure.

27. (Original) A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 6.
28. (Original) A computer program product stored on a computer usable medium, comprising computer readable program means for causing a computer to perform a method according to claim 13.
29. (Cancelled)
30. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for verification, said method steps comprising the steps of claim 1.
31. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for receipt generation, said method steps comprising the steps of claim 6.

32. (Original) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for proving ownership of a receipt, said method steps comprising the steps of claim 13.
33. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing receipt verification, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 24.
34. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing receipt generation, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 25.
35. (Original) A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing proof of receipt ownership, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of the device in claim 26.

IX. EVIDENCE APPENDIX

None. No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of 37 CFR, or any other evidence entered by the Examiner and relied on by Appellant in this appeal.

X. RELATED PROCEEDINGS APPENDIX

None. There have been no decisions rendered by a Court or the Board in any proceeding identified pursuant to 37 CFR 41.37, paragraph (c)(1)(ii) relating to this application.